|  |  |
| --- | --- |
|  | |
|  |  |
|  |  |
| Система защиты персональных данных однопользовательских, подключенных к сетям связи общего пользования, и многопользовательских ИСПДн класса К2, подключенных и не подключенных к сетям связи общего пользования  (шифр: Т2.ПГ2)  ТИПОВОЕ ТЕХНИЧЕСКОЕ ЗАДАНИЕ  На 25 листах  Действует с \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |
|  |  |
|  | |

**Техническое задание  
на оказание услуг по созданию системы защиты персональных данных**

**и аттестации автоматизированных рабочих мест в администрации**

**Пушкинского муниципального района Московской области**

Содержание

[1 Общие сведения 3](#__RefHeading___Toc239074221)

[2 Назначение и цели создания СЗПДн 6](#__RefHeading___Toc239074222)

[2.1 Назначение СЗПДн 6](#__RefHeading___Toc239074223)

[2.2 Цели создания СЗПДн 6](#__RefHeading___Toc239074224)

[3 Характеристика объекта защиты 7](#__RefHeading___Toc239074225)

[4 Требования к СЗПДн 9](#__RefHeading___Toc239074226)

[4.1 Требования к СЗПДн в целом 9](#__RefHeading___Toc239074227)

[4.1.1 Требования к структуре и функционированию 9](#__RefHeading___Toc239074228)

[4.1.2 Требования к численности и квалификации персонала, режиму его работы 10](#__RefHeading___Toc239074229)

[4.1.3 Показатели назначения 10](#__RefHeading___Toc239074230)

[4.1.4 Требования к надежности 10](#__RefHeading___Toc239074231)

[4.1.5 Требования безопасности 10](#__RefHeading___Toc239074232)

[4.1.6 Требования к эргономике и технической эстетике 10](#__RefHeading___Toc239074233)

[4.1.7 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн 11](#__RefHeading___Toc239074234)

[4.1.8 Требования по сохранности информации при авариях 11](#__RefHeading___Toc239074235)

[4.1.9 Требования к защите от влияния внешних воздействий 11](#__RefHeading___Toc239074236)

[4.1.10 Требования к патентной чистоте 12](#__RefHeading___Toc239074237)

[4.1.11 Требования по стандартизации и унификации 12](#__RefHeading___Toc239074238)

[4.1.12 Требования к размещению технических средств 12](#__RefHeading___Toc239074239)

[4.2 Требования к функциям, выполняемым СЗПДн 12](#__RefHeading___Toc239074240)

[4.2.1 Требования к подсистеме управления доступом 12](#__RefHeading___Toc239074241)

[4.2.2 Требования к подсистеме регистрации и учета 14](#__RefHeading___Toc239074242)

[4.2.3 Требования к подсистеме обеспечения целостности 15](#__RefHeading___Toc239074243)

[4.2.4 Требования к подсистеме антивирусной защиты 16](#__RefHeading___Toc239074244)

[4.2.5 Требования к подсистеме обнаружения вторжений 16](#__RefHeading___Toc239074245)

[4.2.5 Требования к подсистеме криптографической защиты 16](#__RefHeading___Toc239074246)

[4.3 Требования к видам обеспечения 17](#__RefHeading___Toc239074247)

[4.3.1 Требования к программному обеспечению 17](#__RefHeading___Toc239074248)

[4.3.2 Требования к техническому обеспечению 17](#__RefHeading___Toc239074249)

[4.3.3 Требования к организационному обеспечению 17](#__RefHeading___Toc239074250)

[5 Состав и содержание работ по созданию СЗПДн 18](#__RefHeading___Toc239074251)

[6 Порядок контроля и приемки 21](#__RefHeading___Toc239074252)

[7 Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу СЗПДн в действие 22](#__RefHeading___Toc239074253)

[8 Требования к документированию 23](#__RefHeading___Toc239074254)

[9 Источники разработки 24](#__RefHeading___Toc239074255)

[10 Перечень принятых сокращений 25](#__RefHeading___Toc239074256)

# Общие сведения

* 1. Настоящее типовое техническое задание разработано для типовых ИСПДн и описывает требования к Системе защиты персональных данных класса К2 однопользовательских, подключенных к сетям общего пользования ИСПДн, а также многопользовательских ИСПДн, подключенных/не подключенных к сетям общего пользования.
  2. На предпроектной стадии создания системы защиты персональных данных настоящее типовое техническое задание (ТТЗ) должно быть уточнено путем разработки Частного технического задания (ЧТЗ), учитывающего специфику конкретной системы обработки персональных данных.
  3. Разработка ЧТЗ осуществляется на основании разрабатываемой (либо существующей) Модели угроз.
  4. Полное наименование и обозначение системы: Система защиты персональных данных однопользовательских, подключенных к сетям связи общего пользования (далее – ССОП), и многопользовательских ИСПДн класса К2, подключенных или не подключенных к ССОП.
  5. Сокращенное наименование системы: СЗПДн.
  6. Шифр разработки: Т2.ПГ2.
  7. Государственный заказчик: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  8. Пользователь: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  9. Исполнитель: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  10. Работы по созданию СЗПДн проводятся на основании следующих документов:

Государственный контракт на создание СЗПДн;

ЧТЗ на создание СЗПДн;

Требования нормативной и организационно-распорядительной документации.

* 1. Плановый срок начала работ – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
  2. Плановый срок завершения работ – \_\_\_\_\_\_\_\_\_\_\_\_\_
  3. Финансирование работ осуществляется поэтапно в соответствии с Государственным контрактом, заключенным между Государственным заказчиком и Исполнителем работ.
  4. По завершении этапов работ Исполнитель предъявляет Государственному заказчику и Пользователю комплект документации, предусмотренной настоящим ТТЗ, и акты сдачи-приемки научно-технической продукции для проведения приемки.
  5. Порядок оформления и предъявления Государственному заказчику и Пользователю результатов работ определяется на основании действующих стандартов и договорных документов между Государственным заказчиком и Исполнителем.
  6. При разработке ТТЗ использовались следующие нормативно-технические документы и методические материалы:

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Постановление Правительства РФ от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства РФ № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

Приказ Гостехкомиссии России от 30 августа 2002 г. № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»;

Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»;

Приказ № 154 Федеральной службы по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия от 28.04.2008 «Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных»;

Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение ПКЗ-2005)»;

Приказ ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных персональных данных»;

Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/5-144 «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»;

Руководящий документ ФСБ России от 21 февраля 2008 г. № 149/6/6-622 «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»;

Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;

Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;

РД 50-34.698-90 «Автоматизированные системы. Требования к содержанию документов»;

ГОСТ 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;

ГОСТ 34.201-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;

ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

# Назначение и цели создания СЗПДн

## Назначение СЗПДн

* + 1. Назначением СЗПДн является обеспечение информационной безопасности (ИБ) персональных данных (ПДн), обрабатываемых в информационной системе персональных данных (ИСПДн).
    2. СЗПДн призвана обеспечить конфиденциальность ПДн при их обработке в ИСПДн.
    3. Объектом защиты СЗПДн является ИСПДн, описание которой приведено в разделе 2.2.5 настоящего ТТЗ.

## Цели создания СЗПДн

* + 1. Целями создания СЗПДн являются:
* обеспечение защищенности ИСПДн в процессе обработки и хранения ПДн, а также обеспечение конфиденциальности ПДн при их обработке;
* соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК России и ФСБ России.
  + 1. В результате создания СЗПДн должно быть обеспечено:
* снижение вероятности реализации актуальных угроз несанкционированного доступа (НСД) к ПДн (методика определения вероятности реализации угроз приведена в РД ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»);
* определение подлинности субъекта доступа.
  + 1. Критериями оценки достижения поставленных целей по созданию СЗПДн являются:
* соответствие требованиям по обеспечению безопасности ПДн в ИСПДн класса К2, определенным в приказе ФСТЭК России от 5 февраля 2010 г. № 58 «Об утверждении положения о методах и способах защиты информации в информационных персональных данных»;
* выполнение функциональных требований настоящего ТТЗ.
  + 1. Класс ИСПДн может быть пересмотрен по результатам предпроектного обследования объекта защиты, включающего в себя разработку и согласование с Пользователем Модели угроз.
    2. Подтверждением соответствия достигнутых результатов заданным целям в рамках настоящего ТТЗ является аттестация ИСПДн на соответствие требованиям безопасности информации.

# Характеристика объекта защиты

* 1. Объектом защиты являются ПДн, обрабатываемые в типовой ИСПДн, однопользовательской и подключенной к сетям связи общего пользования либо многопользовательской как подключенной, так и не подключенной к сетям связи общего пользования.
  2. Обработка ПДн в ИСПДн осуществляется с использованием средств автоматизации.
  3. ИСПДн может включать в свой состав:

выделенное автоматизированное рабочее место (АРМ), подключенное к ССОП;

комплекс АРМ и (или) локальные информационные системы, состоящие из модулей и (при необходимости) центральной части, расположенные на разных территориально удаленных площадках, объединенных каналами связи в единую информационную систему.

* 1. В рассматриваемой ИСПДн обрабатываются ПДн категории 2 или 3, т.е. данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, либо данные, позволяющие лишь идентифицировать субъекта персональных данных.
  2. Для ПДн категории 2 объем одновременно обрабатываемых ПДн в информационной системе должен включать в себя сведения от 1000 до 100 000 субъектах ПДн субъектах ПДн или персональный данные органа государственной власти проживающих в пределах муниципального образования.
  3. Для ПДн категории 3 объем одновременно обрабатываемых ПДн в информационной системе должен включать в себя сведения о менее чем 1000 субъектах ПДн или персональные данные субъектов в пределах одной организации.
  4. ИСПДн относится к типовым, так как:

обеспечивается только одна характеристика безопасности ПДн – конфиденциальность;

не предусмотрено принятие решений исключительно на основании автоматизированной обработки персональных данных, решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права или законные интересы;

не обрабатываются данные, касающиеся состояния здоровья субъектов персональных данных.

* 1. По структуре ИСПДн относится к распределенным или локальным.
  2. По наличию подключений ИСПДн относится к подключенным или к не подключенным к сетям общего пользования и международного информационного обмена.
  3. По режиму обработки ПДн в ИСПДн система является многопользовательской или однопользовательской.
  4. По разграничению прав доступа ИСПДн относится к системам с разграничением прав доступа, при этом в многопользовательских ИСПДн используются разные права доступа к ПДн для разных пользователей.
  5. Все технические средства ИСПДн находятся на территории Российской Федерации.
  6. Актуальные угрозы ИБ, которым подвержена ИСПДн, определяются и обосновываются в Модели угроз, разрабатываемой Исполнителем на этапе проектирования ИСПДн.
  7. Модель угроз разрабатывается на основе Руководящего документа ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
  8. ИСПДн принадлежит к классу К2 в соответствии с совместным приказом ФСТЭК России, ФСБ России и Мининформсвязи России от 13 февраля 2008 г. № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных».

# Требования к СЗПДн

## Требования к СЗПДн в целом

### Требования к структуре и функционированию

* + - 1. В состав СЗПДн должны входить следующие подсистемы:

 управления доступом;

 регистрации и учета;

 обеспечения целостности;

 антивирусной защиты;

 обнаружения вторжений;

 обеспечения межсетевой безопасности;

 анализа защищенности.

* + - 1. Структура СЗПДн может изменяться и уточняться по результатам разработки Модели угроз на предпроектной стадии с учетом обоснования необходимых изменений в ЧТЗ.
      2. **Подсистема управления доступом** должна проводить процедуру проверки подлинности пользователя, его авторизации, разграничивать доступ пользователей к ресурсам ИСПДн.
      3. **Подсистема регистрации и учета** должна обеспечивать регистрацию действий пользователей при работе с ресурсами ИСПДн и учет событий ИБ.
      4. **Подсистема обеспечения целостности** должна обеспечивать контроль неизменности состояния рабочей среды пользователей при работе на АРМ, системных файлов ОС серверной части ИСПДн и СЗИ, используемых в СЗПДн, а также обеспечивать анализ защищенности системного и прикладного программного обеспечения ИСПДн с помощью программных средств или программно-аппаратных средств анализа защищенности (САЗ).
      5. **Подсистема антивирусной защиты** должна осуществлять защиту информационных ресурсов ИСПДн от внедрения вредоносного ПО.
      6. Подсистема антивирусной защиты должна минимизировать угрозы внедрения вредоносного ПО в СЗИ, ОС и общесистемное ПО, определенные Моделью угроз как актуальные.
      7. Требования к **подсистеме обнаружения вторжений** предъявляются для информационных систем, подключенных к сетям международного информационного обмена и к сетям общего пользования и обеспечиваются путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений.
      8. **Подсистема анализа защищенности** должна обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.
      9. Требования к **подсистеме обеспечения межсетевой безопасности** предъявляются для информационных систем, подключенных к сетям международного информационного обмена и к сетям общего пользования и обеспечиваются использованием межсетевых экранов.

### Требования к численности и квалификации персонала, режиму его работы

* + - 1. Квалификация персонала должна быть достаточной для осуществления им настройки общесистемных и сетевых сервисов СЗПДн и настройки СЗИ СЗПДн.
      2. Персонал СЗПДн должен осуществлять обслуживание и эксплуатацию СЗПДн по рабочим дням в рабочее время с возможностью выхода в нерабочее время для проведения сервисного обслуживания или восстановления работоспособности СЗПДн.

### Показатели назначения

* + - 1. Системно-технические решения СЗПДн должны обеспечить минимизацию вероятности реализации угроз, описанных в Модели угроз для данной ИСПДн.
      2. Экономический эффект от создания СЗПДн должен проявляться в снижении вероятной величины материального и морального ущерба по отношению к субъектам и оператору ПДн.

### Требования к надежности

* + - 1. Аппаратно-программные компоненты СЗПДн должны удовлетворять условию круглосуточной работы, позволять осуществлять резервирование и восстановление системы после сбоев.
      2. Должна быть обеспечена возможность резервного копирования конфигураций и журналов регистрации событий компонентов СЗПДн.

### Требования безопасности

* + - 1. В процессе обслуживания и эксплуатации оборудования СЗПДн должна обеспечиваться безопасность персонала.
      2. Конструкция используемого оборудования должна обеспечивать защиту эксплуатирующего персонала от поражения электрическим током в соответствии с требованиями ГОСТ 12.2.003 и ГОСТ 12.2.007.
      3. Размещение оборудования на штатных местах должно обеспечивать его безопасное обслуживание и эксплуатацию.

### Требования к эргономике и технической эстетике

* + - 1. Серверные компоненты и активное сетевое оборудование СЗПДн должны иметь возможность установки в монтажные стойки, предоставленные для размещения оборудования системы.
      2. АРМ администратора, входящее в состав СЗПДн, должно отвечать требованиям ГОСТ 27201-87 «Машины вычислительные электронные персональные. Типы, основные параметры, общие технические требования».
      3. АРМ администратора СЗПДн должно обеспечивать возможность непрерывной работы операторов в течение смены в соответствии с требованиями Постановления Главного государственного санитарного врача РФ от 3 июня 2003 г. № 118 «О введении в действие санитарно-эпидемиологических правил и нормативов СанПиН 2.2.2/2.4.1340-03» с изменениями от 25 апреля 2007 г.

### Требования к эксплуатации, техническому обслуживанию, ремонту и хранению компонентов СЗПДн

* + - 1. При создании СЗПДн должны использоваться унифицированные, однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, удобства эксплуатации.
      2. Климатические условия эксплуатации компонентов СЗПДн должны соответствовать требованиям ГОСТ 21552-84 и ГОСТ 27201-87.
      3. Эксплуатация программно-технических средств должна предусматривать следующие виды технического обслуживания:

оперативное обслуживание,

профилактические работы.

* + - 1. Оперативное обслуживание должно предусматривать ежедневный контроль функционирования аппаратно-технических средств, целостности ресурсов системы. Оперативное обслуживание не должно нарушать выполнения функций СЗПДн в целом.
      2. Профилактическое обслуживание должно предусматривать периодическую проверку и обслуживание составных частей СЗПДн, для которых такое обслуживание предусмотрено эксплуатационной документацией.
      3. Объем и порядок выполнения технического обслуживания технических и программных средств СЗПДн должны определяться эксплуатационной документацией.
      4. Физический доступ неуполномоченных лиц к сетевому и серверному оборудованию должен быть запрещен.
      5. Требования к эксплуатации, техническому обслуживанию, ремонту и хранению могут уточняться на этапе проектирования СЗПДн.

### Требования по сохранности информации при авариях

* + - 1. Сохранность информации при авариях в СЗПДн должна обеспечиваться методом резервного копирования.
      2. Решения по обеспечению сохранности информации в СЗПДн при авариях должны быть разработаны на стадии технорабочего проекта.

### Требования к защите от влияния внешних воздействий

* + - 1. Защита ИСПДн от влияния внешних воздействий должна осуществляться в рамках общих организационно-технических мероприятий по обеспечению безопасности и физической защите на объектах Пользователя.
      2. В рамках СЗПДн должны использоваться средства вычислительной техники, удовлетворяющие требованиям стандартов Российской Федерации и требованиям Госкомсвязи России «Автоматизированные системы управления аппаратурой электросвязи», 1998 г. по электромагнитной совместимости и помехозащищенности.

### Требования к патентной чистоте

* + - 1. При создании СЗПДн должны соблюдаться положения законодательных актов Российской Федерации по соблюдению авторских прав и защите специальных знаков.
      2. При поставке программного обеспечения должны быть выполнены требования Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.92 г., а также международные патентные соглашения.

### Требования по стандартизации и унификации

* + - 1. Решения по использованию технических средств и ПО в СЗПДн должны использовать однотипные компоненты в целях обеспечения снижения расходов на обслуживание и ремонт, взаимозаменяемости используемых компонентов, удобства эксплуатации.
      2. Должна обеспечиваться совместимость технических средств и ПО СЗПДн с техническими средствами и ПО, используемыми в ИСПДн.
      3. При применении технических средств и ПО особое внимание должно быть уделено унификации программных и аппаратных решений. Предпочтение должно отдаваться использованию готовых, проверенных на практике решений.

### Требования к размещению технических средств

* + - 1. Серверное оборудование СЗПДн и телекоммуникационное оборудование должны размещаться в выделенном помещении.
      2. Серверное оборудование, входящее в состав СЗПДн, и телекоммуникационное оборудование должны иметь возможность установки в отдельный монтажный шкаф.
      3. Серверы и телекоммуникационное оборудование ИСПДн должны располагаться в отдельном помещении. В случае если это невозможно, средства и телекоммуникационное оборудование ИСПДн должны находиться в отдельном запираемом монтажном шкафу (шкафах).

## Требования к функциям, выполняемым СЗПДн

**5.4.1 Для ИСПДн 2 класса при однопользовательском режиме обработки ПДн должны выполняться следующие функции:**

**5.4.1.1 в подсистеме управления доступом:**

* должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

**5.4.1.2 в подсистеме регистрации и учета:**

* должна осуществляться регистрация входа (выхода) субъекта доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
* должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);

**5.4.1.3 в подсистеме обеспечения целостности:**

* должна быть обеспечена целостность программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность программных средств проверяется при загрузке системы по наличию имен (идентификаторов) компонентов системы защиты персональных данных, целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;
* должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;
* должно проводиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;
* должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль

**5.4.1.4 в подсистеме антивирусной защиты:**

* в соответствии с пунктом 2.4 «Положения о методах и способах защиты информации в информационных системах персональных данных» в СЗПДн должны использоваться средства антивирусной защиты.

**5.4.1.5 в подсистеме межсетевой безопасности:**

МЭ должен обеспечивать:

* должна осуществляться фильтрация на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* должна осуществляться фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* должна осуществляться фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* должна осуществляться фильтрация с учетом любых значимых полей сетевых пакетов;
* должна осуществляться регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
* должна осуществляться идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
* должна осуществляться регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* должна осуществляться регистрация запуска программ и процессов (заданий, задач);
* должен осуществляться контроль целостности своей программной и информационной части;
* должен обеспечиваться восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* должна проводится регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

**5.4.1.6 в подсистеме обнаружения и предотвращения вторжений:**

* обнаружение вторжений проводится путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений и обеспечивает обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных.

**5.4.1.7 в подсистеме анализа защищенности:**

* средства (система) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

**5.4.2 Для ИСПДн 2 класса при многопользовательском режиме обработки ПДн и равными правами доступа к ним разных пользователей должны выполняться следующие функции:**

**5.4.2.1 в подсистеме управления доступом:**

* должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;

**5.4.2.2 в подсистеме регистрации и учета:**

* должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная);
* должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

**5.4.2.3 в подсистеме обеспечения целостности:**

* должно осуществляться обеспечение целостности программных средств системы защиты персональных данных, обрабатываемой информации, а также неизменность программной среды. При этом целостность системы защиты персональных данных проверяется при загрузке системы по наличию имен (идентификаторов) ее компонент, а целостность программной среды обеспечивается отсутствием в информационной системе средств разработки и отладки программ;
* должна осуществляться физическая охрана технических средств информационной системы (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания;
* должно осуществляться периодическое тестирование функций системы защиты персональных данных при изменении программной среды и пользователей информационной системы с помощью тест-программ, имитирующих попытки несанкционированного доступа;
* необходимо наличие средств восстановления системы защиты персональных данных, предусматривающих ведение двух копий программных компонентов средств защиты информации, их периодическое обновление и контроль работоспособности.

**5.4.2.4 в подсистеме антивирусной защиты:**

* в соответствии с пунктом 2.4 «Положения о методах и способах защиты информации в информационных системах персональных данных» в СЗПДн должны использоваться средства антивирусной защиты.

**5.4.2.5 в подсистеме межсетевой безопасности:**

МЭ должен обеспечивать:

* должна осуществляться фильтрация на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* должна осуществляться фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* должна осуществляться фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* должна осуществляться фильтрация с учетом любых значимых полей сетевых пакетов;
* должна осуществляться регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
* должна осуществляться идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
* должна осуществляться регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* должна осуществляться регистрация запуска программ и процессов (заданий, задач);
* должен осуществляться контроль целостности своей программной и информационной части;
* должен обеспечиваться восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* должна проводится регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

**5.4.2.6 в подсистеме обнаружения и предотвращения вторжений:**

* обнаружение вторжений проводится путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений и обеспечивает обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных.

**5.4.2.7 в подсистеме анализа защищенности:**

* средства (система) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

**5.4.3** **Для ИСПДн 2 класса при многопользовательском режиме обработки ПДн и разными правами доступа к ним разных пользователей должны выполняться следующие функции:**

**5.4.3.1 в подсистеме управления доступом:**

* должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длинной не мене шести буквенно-цифровых символов.

**5.4.3.2 в подсистеме регистрации и учета:**

* должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы, результат попытки входа (успешная или неуспешная - несанкционированная), идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
* должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);

**5.4.3.3 в подсистеме обеспечение целостности:**

* должна быть обеспечена целостность программных средств защиты информации в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по контрольным суммам компонент средств защиты информации, а целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
* должна осуществляться физическая охрана ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации, особенно в нерабочее время;
* должно проводиться периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест - программ, имитирующих попытки НСД;
* должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;

**5.4.3.4 в подсистеме антивирусной защиты:**

* в соответствии с пунктом 2.4 «Положения о методах и способах защиты информации в информационных системах персональных данных» в СЗПДн должны использоваться средства антивирусной защиты.

**5.4.3.5 в подсистеме межсетевой безопасности:**

МЭ должен обеспечивать:

* должна осуществляться фильтрация на сетевом уровне независимо для каждого сетевого пакета (решение о фильтрации принимается на основе сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов);
* должна осуществляться фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
* должна осуществляться фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;
* должна осуществляться фильтрация с учетом любых значимых полей сетевых пакетов;
* должна осуществляться регистрация и учет фильтруемых пакетов (в параметры регистрации включаются адрес, время и результат фильтрации);
* должна осуществляться идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ по идентификатору (коду) и паролю условно-постоянного действия;
* должна осуществляться регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузки и инициализации системы и ее программного останова (регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана);
* должна осуществляться регистрация запуска программ и процессов (заданий, задач);
* должен осуществляться контроль целостности своей программной и информационной части;
* должен обеспечиваться восстановление свойств межсетевого экрана после сбоев и отказов оборудования;
* должна проводится регламентное тестирование реализации правил фильтрации, процесса регистрации, процесса идентификации и аутентификации администратора межсетевого экрана, процесса регистрации действий администратора межсетевого экрана, процесса контроля за целостностью программной и информационной части, процедуры восстановления.

**5.4.3.6 в подсистеме обнаружения и предотвращения вторжений:**

* обнаружение вторжений проводится путем использования в составе информационной системы программных или программно-аппаратных средств (систем) обнаружения вторжений и обеспечивает обнаружение вторжений в информационную систему, нарушающих или создающих предпосылки к нарушению установленных требований по обеспечению безопасности персональных данных.

**5.4.3.7 в подсистеме анализа защищенности:**

* средства (система) анализа защищенности должны обеспечивать возможность выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения информационной системы, которые могут быть использованы нарушителем для реализации атаки на систему.

Для обеспечения безопасности персональных данных при удаленном доступе к информационной системе через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо указанных методов и способов, дополнительно необходимо применять следующие методы и способы защиты информации от несанкционированного доступа несанкционированного доступа:

* проверка подлинности отправителя (удаленного пользователя) и целостности передаваемых по информационно-телекоммуникационной сети международного информационного обмена (сети связи общего пользования) данных;
* управление доступом к защищаемым персональным данным информационной сети;
* использование атрибутов безопасности.

Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо указанных методов и способов, дополнительно необходимо применять следующие методы и способы защиты информации от несанкционированного доступа несанкционированного доступа:

* создание канала связи, обеспечивающего защиту передаваемой информации;
* осуществление аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных.

Для обеспечения безопасности персональных данных при межсетевом взаимодействии отдельных информационных систем разных операторов через информационно-телекоммуникационную сеть международного информационного обмена (сеть связи общего пользования) помимо методов и способов, дополнительно необходимо применять следующие методы и способы защиты информации от несанкционированного доступа несанкционированного доступа:

* создание канала связи, обеспечивающего защиту передаваемой информации;
* аутентификация взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;
* обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;
* обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя.

## Требования к видам обеспечения

### Требования к программному обеспечению

* + - 1. Выбор программных средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у Пользователя.
      2. Должны использоваться средства защиты информации от НСД, сертифицированные в ФСТЭК России.
      3. В случае, когда в состав СЗПДн включается подсистема криптографической защиты, должны использоваться криптосредства, сертифицированные в ФСБ России.
      4. При создании СЗПДн должно использоваться только лицензионное общее и специальное программное обеспечение и операционные системы.
      5. Требования к программному обеспечению, используемому для защиты информации в ИСПДн (средств защиты информации, в том числе и встроенных в общесистемное и прикладное ПО) в части необходимости обеспечения контроля отсутствия в нем недекларированных возможностей (НДВ) должны быть определены в ЧТЗ.

### Требования к техническому обеспечению

* + - 1. Выбор аппаратных (программно-аппаратных) средств защиты должен проводиться с учетом средств защиты, эксплуатируемых у Пользователя.
      2. Аппаратные компоненты должны обеспечивать функции диагностики, резервирования и взаимозаменяемости.

### Требования к организационному обеспечению

* + - 1. Должна осуществляться физическая охрана помещений, в которых находятся средства ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения и хранилище носителей информации, особенно в нерабочее время.
      2. Мониторы АРМ должны располагаться таким образом, чтобы препятствовать возможности несанкционированного визуального съема информации с них.
      3. Должны быть реализованы мероприятия по защите ПДн от утечки за счет побочных электромагнитных излучений и наводок.

# Состав и содержание работ по созданию СЗПДн

* 1. Работы по созданию СЗПДн осуществляют по стадиям и этапам:

Предпроектная стадия:

обследование ИСПДн;

классификация ИСПДн;

разработка Модели угроз;

разработка Частного технического задания (ЧТЗ) на создание СЗПДн.

Технорабочий проект:

разработка Технорабочего проекта СЗПДн;

разработка эксплуатационной документации (в случае необходимости);

разработка организационно-распорядительной документации (в случае необходимости).

Ввод в действие:

поставка оборудования и ПО согласно спецификации, разработанной на этапе проектирования;

монтаж оборудования, установка и настройка ПО в соответствии с проектными решениями;

предварительные испытания и ввод в опытную эксплуатацию;

опытная эксплуатация средств защиты информации в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;

доработка СЗПДн по результатам опытной эксплуатации (при необходимости).

аттестация ИСПДн:

разработка аттестационной документации;

оценка соответствия ИСПДн требованиям безопасности;

проведение аттестационных мероприятий ИСПДн;

приемочные испытания и перевод ИСПДн в промышленную эксплуатацию.

* 1. На предпроектной стадии проводится обследование ИСПДн:

уточняется перечень ПДн, подлежащих защите;

уточняется информация о категориях и составе ПДн, обрабатываемых автоматизированными и неавтоматизированными способами; проводится анализ состава ПДн в ИСПДн, собирается информация о защищенности ПДн;

уточняются условия расположения объекта защиты относительно границ контролируемой зоны;

уточняются конфигурация и топология ИСПДн и систем связи в целом и их компонентов, физические, функциональные и технологические связи как внутри этих систем, так и с другими системами различного уровня и назначения;

уточняются состав технических средств и систем, предполагаемых к использованию в СЗПДн, условия их расположения, общесистемные и прикладные программные средства;

уточняются режимы обработки информации в ИСПДн в целом и в отдельных ее компонентах; для ИСПДн производится анализ собранной информации об угрозах и их показателях для разработки Модели угроз;

уточняется класс ИСПДн;

разрабатывается Модель угроз для ИСПДн на основе методических рекомендаций ФСТЭК России, а также Модель нарушителя (в случае необходимости) на основе методических рекомендаций ФСБ России;

уточняется степень участия сотрудников в обработке информации, характер их взаимодействия между собой и со службой ИБ;

разрабатывается ЧТЗ на создание СЗПДн.

* 1. По результатам проведенных работ по обследованию ИСПДн в дополнение к настоящему ТТЗ разрабатывается ЧТЗ с детальными требованиями к СЗПДн.
  2. При разработке ЧТЗ формируется перечень документации, разрабатываемой на стадии технорабочего проекта.
  3. На стадии технорабочего проекта разрабатывается документация согласно ЧТЗ, при этом содержание документов должно соответствовать требованиям РД 50-34.698-90.
  4. На стадии ввода в действие выполняются следующие работы:

поставка оборудования и ПО на площадку Пользователя согласно спецификации, разработанной на стадии технорабочего проекта;

монтаж оборудования, установка и настройка ПО в соответствии с проектными решениями;

опытная эксплуатация СЗИ СЗПДн в комплексе с другими техническими и программными средствами в целях проверки их работоспособности в составе объекта информатизации и отработки технологического процесса обработки (передачи) информации;

доработка СЗПДн по результатам опытной эксплуатации (при необходимости);

инструктаж персонала Пользователя по работе с основными компонентами СЗПДн;

в случае необходимости проводится обучение персонала Пользователя использованию СЗИ, применяемых в СЗПДн.

* 1. На этапе аттестации проводятся мероприятия по получению аттестата соответствия ИСПДн требованиям безопасности ПДн, предъявляемым к классу К2.
  2. Аттестация по требованиям безопасности информации предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса, используемого на конкретном объекте информатизации.
  3. Под аттестацией объекта автоматизации понимается комплекс организационно-технических мероприятий, в результате которых специальным документом – Аттестатом соответствия подтверждается, что объект соответствует требованиям стандартов и нормативно-техническим документам (в том числе по безопасности ПДн), утвержденным ФСТЭК России.
  4. Аттестационные испытания ИСПДн на соответствие требованиям РД ФСТЭК России проводятся в два подэтапа:

1. Разработка пакета аттестационных документов.

Подготовка и проведение аттестационных испытаний.

* 1. По окончании аттестационных испытаний ИСПДн оформляется комплект отчетных документов, необходимых для получения аттестата соответствия.
  2. После получения аттестата соответствия проводятся приемочные испытания с целью перевода ИСПДн в промышленную эксплуатацию. Акт о приемке системы в промышленную эксплуатацию должен быть подписан Государственным заказчиком, Пользователем и Исполнителем.
  3. Стадии проведения работ по созданию СЗПДн приведены в Табл. 1.

Табл. 1 – Стадии создания СЗПДн

| № | Наименование стадии | Сроки начала работ | Сроки окончания работ | Результат |
| --- | --- | --- | --- | --- |
| 1 | Предпроектная стадия |  |  | Разработанное ЧТЗ |
| 2 | Технорабочий проект |  |  | Техническая, рабочая и другая документация |
| 3 | Ввод в действие |  |  | Акт сдачи ИСПДн в промышленную эксплуатацию |

* 1. Стадии создания СЗПДн должны соответствовать требованиям ГОСТ 34.601-90 «Автоматизированные системы. Стадии создания».

# Порядок контроля и приемки

* 1. Контроль и приемка работ осуществляются на основании ЧТЗ и соответствующих программ и методик испытаний.
  2. Содержание отчетных материалов согласуется на уровне специалистов Государственного заказчика, Пользователя и Исполнителя в соответствии с ЧТЗ. Исполнитель должен быть заранее проинформирован Государственным заказчиком и Пользователем о порядке и сроках согласования отчетных материалов, перечне вопросов, которые подлежат согласованию, составе согласующих подразделений и организаций и степени их компетенции при согласовании тех или иных разделов отчетной документации.
  3. В случае необходимости может быть проведена защита предлагаемых решений в процессе технического совещания специалистов Исполнителя и Пользователя.
  4. Настоящее ТТЗ может быть уточнено или изменено в процессе работы. Уточнения и изменения ТТЗ производятся по согласованию сторон. Оформление изменений осуществляется выпуском дополнений, которые являются неотъемлемой частью настоящего ТТЗ.
  5. Согласование и утверждение изменений производится в том же порядке и теми же должностными лицами, что и согласование и утверждение ТТЗ.
  6. Замечания по отчетным материалам должны быть представлены Исполнителю с техническим обоснованием в письменной форме.
  7. Виды, состав, объем и методы испытаний СЗПДн и ее частей определяются программой и методикой испытаний.
  8. Испытания проводятся на площадках развертывания СЗПДн.
  9. Сроки приемки работ определяются календарными планами и сроками проведения соответствующих этапов в соответствии с техническими требованиями на создание СЗПДн.
  10. Прием и сдача проводимых работ осуществляются совместной комиссией на основе утвержденной программы и методики испытаний.

# Требования к составу и содержанию работ по подготовке объекта автоматизации к вводу СЗПДн в действие

* 1. Реализация требований настоящего раздела не входит в перечень работ, выполняемых Исполнителем в рамках создания СЗПДн. Данные требования должны быть реализованы Пользователем.
  2. На этапе ввода СЗПДн должен быть определен перечень лиц допущенных к обработке ПДн, обрабатываемых в ИСПДн.
  3. Должен быть определен перечень информации, классифицируемой как ПДн.
  4. Разграничение прав доступа в серверные помещения должно регламентироваться внутренними организационно-распорядительными документами Пользователя.
  5. Компоненты СЗПДн, в том числе телекоммуникационное оборудование, должны быть подключены к источникам бесперебойного питания.
  6. Серверное помещение должно быть оборудовано средствами вентиляции и кондиционирования воздуха, достаточными для работы оборудования в соответствии с документацией производителя, а также средствами автоматического пожаротушения и пожарной сигнализации.

# Требования к документированию

* 1. На стадии технорабочего проекта рекомендуется выпустить следующий комплект документации:

Ведомость технорабочего проекта;

Пояснительная записка к технорабочему проекту;

Описание технологического процесса обработки данных;

Таблица соединений и подключений;

Чертеж установки технических средств;

План расположения;

Паспорт;

Программа и методика испытаний.

* 1. Окончательный перечень документов, выпускаемых на стадии технорабочего проекта, должен быть определен в ЧТЗ.
  2. Виды, комплектность и содержание документов в части, определенной настоящим ТТЗ, должны учитывать требования ГОСТ 34.201-89 и РД 50-34.698.
  3. Комплект проектных материалов предоставляется Государственному заказчику и Пользователю в электронном виде и на твердой копии (количество экземпляров определяется в ЧТЗ). Вся разрабатываемая проектная документация должна быть выполнена на русском языке.

# Источники разработки

* 1. При разработке проектных решений необходимо руководствоваться официальными документами фирм-производителей применяемых аппаратных средств и программного обеспечения, документами третьих сторон, осуществляющих тестирование и эксплуатацию решений, материалами, предоставляемыми Пользователем.
  2. Проектные решения должны обеспечивать соблюдение следующих федеральных законов, постановлений Правительства Российской Федерации и нормативных актов:

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 08 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности»;

РД Гостехкомиссии России «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники»;

Руководящие документы ФСТЭК России и ФСБ России, регламентирующие мероприятия в области защиты информации.

# Перечень принятых сокращений

|  |  |
| --- | --- |
| АРМ | Автоматизированное рабочее место |
| АС | Автоматизированная система |
| ВП | Вредоносные программы |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| ИСПДн | Информационная система персональных данных |
| МЭ | Межсетевой экран |
| НСД | Несанкционированный доступ |
| ОС | Операционная система |
| ПДн | Персональные данные |
| ПМВ | Программно-математические воздействия |
| ПО | Программное обеспечение |
| ПЭМИН | Побочные электромагнитные излучения и наводки |
| РД | Руководящий документ |
| САЗ | Средства анализа защищенности |
| СЗИ | Средство защиты информации |
| СЗПДн | Система защиты персональных данных |
| ССОП | Сеть связи общего пользования |
| СУБД | Система управления базами данных |
| ТТЗ | Типовое техническое задание |
| ФЗ | Федеральный закон |
| ЧТЗ | Частное техническое задание |

СОСТАВИЛИ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации | Должность | Фамилия, Имя, Отчество | Подпись | Дата |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

СОГЛАСОВАНО

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Наименование организации | Должность | Фамилия, Имя, Отчество | Подпись | Дата |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |